Initial Documentation Requirements for a High Assurance System: Lessons Learned

Paul C. Clark, Cynthia E. Irvine, *Senior Member, IEEE*, Timothy E. Levin, *Member, IEEE*,
Thuy D. Nguyen, David J. Shifflett, Donna Miller
Naval Postgraduate School

833 Dyer Rd., Code CS/Cp
Monterey, CA 93943-5118
(831) 656-2395
Fax: (831) 656-2814
pcclark@nps.edu

I. Introduction

The Center for Information Systems Security Studies and Research (CISR) is working on the Trusted Computing Exemplar (TCX)project[-], which "will provide an openly distributed worked example of how high assurance trusted computing components can be built" [1]. One of these components is a small separation kernel that can enforce process and data separation. In addition, a reference trusted application will be built to use this kernel [2].

The motivation for the TCX project is the fact that few high assurance systems have ever been successfully completed or evaluated, and of these, they have all been proprietary. Thus, it is extremely difficult for those new to information assurance to learn how to construct high assurance systems. An objective of the TCX project is to provide the information that will allow more organizations to consider building high assurance products. It is intended to remove the "mystery" of high assurance development through a worked example.

The validation that a system is high assurance is provided via an independent third-party evaluation. A key aspect of a high assurance evaluation is the documented methodologies, standards, and processes that are used throughout the product lifecycle. This paper presents the lessons learned to date through the creation of documents required prior to the engineering phase of development.

[-] *This work was sponsored in part by the Office of Naval Research and the National Reconnaissance Office. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of either the Office of Naval Research or the National Reconnaissance Office.*

II. Common Criteria

The Common Criteria (CC) is an internationally recognized standard for security of computing products [3]. It predefines seven different levels of assurance, known as Evaluation Assurance Levels (EALs), where EAL7 is the highest assurance. Each level is comprised of a set of requirements from CC Part 3, where each higher EAL imposes additional constraints or additional new requirements beyond those of the adjacent lower level. Thus, it is recognized that EALs 1 through 4 are "low" assurance levels, while EALs 5 through 7 are "high" assurance levels. To provide the maximum benefit as a worked example, the TCX separation kernel is targeted for an EAL7 evaluation, which drove the documentation decisions described here.

There is no simple or consolidated reference in the CC framework that describes the overall documentation requirements for a given EAL. Instead, documentation requirements are interspersed among all the other assurance requirements, with related requirements sometimes found in different parts of the CC. One must carefully assess all the requirements that map to the desired EAL. Even then, the wording may be vague and must be interpreted. In addition, the semantics of some of the terminology used in the CC differs from that of other standards with which the TCX team was familiar[TCSEC].

In an attempt to minimize the risk of erroneous interpretation, the Common Methodology for Information Technology Security Evaluation (CEM) document was referenced [4]. The CEM document provides guidance to evaluators, and occasionally provides insight into what the authors of the CC intended when they wrote the requirements. However, the CEM only provides guidance

for low assurance evaluations, so for many of the high assurance issues, the CEM was not helpful. In addition, an update to the CC documents during the TCX initial documentation effort added to the difficulty.

III. Required Documents

After studying the CC, it was determined that over 40 documents are required for an EAL7 evaluation. As overwhelming as that may sound, only the following short list of documents had to be in place before the start of development:

- Documentation Standards
- Life Cycle Plan
- Configuration Management Plan
- Configuration Management Procedures
- Configuration Items List
- Personnel Security Plan
- Physical Security Plan
- Software Development Standards

Failure to create such documents prior to system development would render any attempt for a high assurance rating fruitless. They cannot be written post facto as an exercise to fulfill all high assurance requirements, because the opportunity to have them contribute to system assurance is gone. Organizations that hope to receive a high assurance rating for a product must provide evidence that high assurance development practices were actually followed from the beginning of the product lifecycle. Thus, the documentation not only describes what must be done, but also describes how and when evidence shall be created and maintained.

During an evaluation, one of the first things that an evaluator will examine is whether the stated methodologies, policies and standards were good enough to qualify for the desired rating. Once that test is passed, the evaluator will want to see proof that the organization actually adhered to them. Therefore, when writing any of the documents listed above, the author must continually ask the question: "How will I prove that I did all the things I said I was going to do?" In other words, what evidence will be needed to show that the stated methodologies, policies and standards were strictly followed from the start of development?

Another challenge for the developer is knowing what is necessary and sufficient. It is possible to go beyond the mark when considering how to meet all the requirements: to do more than the minimum necessary for the desired rating. The evaluators would normally award the desired rating in such a case, but it will be at a greater cost to the developer than was necessary. Therefore, another question to consider is, "Is this too much?" It was valuable for the TCX documentation effort to have some team members keep asking this question.

The order in which the documents are written is also important. In our experience, the first five documents in the previous list must be created in the order given, with the Documentation Standards written first.

It should also be noted that when the CC describes a documentation requirement, it does not mean that it must be met by a specific separate document – multiple documentation requirements can be met by a single document.

IV. summary

Although there are a large number of documentation requirements for a high assurance CC evaluation, our experience has revealed that only eight documents must be written before development can start. However, for a variety of reasons when starting from scratch, these eight documents require significant effort, especially if one is not familiar with the CC. Careful thought must go into these documents because they form the whole framework for a high assurance environment, and fundamental evidence that a product merits a high assurance rating.

These eight documents, along with other TCX documentation and source code, will be made available to the general public at a future point in time.

V. References

[1] Irvine, Cynthia E., et. al., *The Trusted Computing Exemplar Project*, Proceedings of the 2002 IEEE Workshop on Information Assurance and Security, pgs. 30-36, West Point, NY, June 2002.

[2] Nguyen, Thuy D., et. al., *TCX Project: High Assurance for Secure Embedded Systems*, 11th IEEE Real-Time Embedded Technology and Applications Symposium (presented as a Work-in-Progress), March 2005.

[3] Common Criteria for Information Technology Security Evaluation, version 2.2, January 2004, CCIMB-2004-01-001.

[4] Common Methodology for Information Technology Security Evaluation, version 1.0, August 1999, CEM-99/045.